ISMG Meeting Minutes

Date: August 25, 2011
Time: 1:02 pm
Location: Mitchell building, room 218

Attendees

Pat Boles, SITSD; Kristi Antosh, MDT; Bill Hallinan, TRS; Michael Sweeney, DOA; Dawn Harmon, CSI/SAO; Lynne Pizzini, SITSD; Jim Ashmore, SITSD/CIO Program Office; Kimberly Kessler, COR; Cleo Anderson, DOR; Julie Kriedeman, SITSD and Jaclyn Hardamon, SITSD.

Call to Order – Pat Boles

- Pat Boles called the August meeting to order and asked for introductions.

Approval of Minutes – Pat Boles

- Pat asked for comments or changes to the July minutes.
  **** Action Item****
- **Kristi Antosh** offered a motion to approve the minutes. **Bill Hallinan** seconded.
  - Motion passed unanimously.

Introduction of Security Analyst – Pat Boles

Pat introduced Jim Ashmore as the new Information Security Policy Analyst, SITSD. Jim provided more detail speaking about his background with the military, internal controls, accounting, tribal governments, education, restaurant and food services, security systems and that he was a volunteer firefighter.

Agenda Revision

Lynne asked if Pat can talk about the December IT Conference Topics first as she would have to leave early. So Pat jumped to this topic on the agenda first.

December IT Conference Topics

- The collected list of proposed topics was presented for feedback and priorities. Lynne needs to get speakers lined up soon and wants to confirm topics as soon as possible because there are four or five time slots to fill.
- Bill asked if by the end of the month would work and Lynne agreed that would be fine.
- Kristi asked Lynne if she wanted a 1-9 priority order and Lynne agreed.
- Kristi brought up current threats. She asked Lynne if she wanted the ISMG to identify what they think are the current threats or if this was a generic topic that the speaker would determine the threats to cover? Lynne indicated the latter.
- Kristi also discussed the current and future impact of mobile devices as a security topic.
- There was a discussion of data security in general as a topic.
- Cloud security was also discussed as a "generic" topic.
- Lynne said she is doing a Cloud security presentation at MSU in September.
- Pat asked Lynne to put her presentation on the website.

- Lynne discussed the human factor of security and how the user affects the systems.
- Kristi mentioned Web Application Security and Application Security, passwords and extended security.
- Jim asked, what is training for every State employee, what topics should be covered and how.
- Bill asked about procedural check lists for new or terminating employees.
- Lynne said "Provision" is in place for adding a new employee to the network.
- Dawn said FWP has, in their policy and procedures, a checklist (SFSAR form) which has levels of checklists which need to be reviewed and signed.
- Kristi said her department has steps that are handled by various groups, but it is not in one 'form'.
- Lynne said that ITSD is moving to "Role" based access.
- Bill talked about the legal perspective: sensitive information, code of ethics for new employees and training.
- Pat asked everyone to have their top four or five topics in by end of Friday and then we can start voting on them.

Risk Management Strategy Development – Pat Boles

- Jim clarified a correction on the document and Pat confirmed the typo.
- Pat reviewed and said he added more information about how to evaluate threats, risk identification and methodology, evaluation criteria, risk response guidelines to the document. He opened the topic for discussion.
- Kristi confirmed with Pat that this is a living document that might change your risk management strategy.
- Jim clarified that each organization would take this document and restructure it to their needs. Pat confirmed.
- Pat clarified that no deadline is set. The document is in the August folder. Pat wants all to collaborate and capture as much information as possible. The goal of the Risk Management Strategy Document is to produce a foundation for the Information Risk Management Program. This document becomes an input in how your organization assesses, responds to, and monitors risk. This document provides the ability to develop a plan of responding to and monitoring risk that can be used to ask the legislature to fund the response to agency identified risks. He wants all to identify risks and to then take the document to the Legislature.
- Mike said risk and security is just one aspect. He said he would like to tie it in with other projects. He said security should be taken care of quickly.
- Pat agreed there are multiple aspects.
- Mike said we need to save money and create efficiencies.
- Jim clarified that this is a process that should be integrated within decision making structures.

- Pat said he had not found any other states that had a document like this, only the reference organizations in the UK. He even checked with Norex. Pat spoke about other documents and said it is a great approach but it is more than that, "it is fluid". He said this process is still pretty new as NIST SP 800-39 was only published in March of this year.
- Jim suggested a timeline. He asked if it should be discussed at the December conference. The goal is for June or July 1, 2012.
- Timelines and deadlines were discussed for agencies
- Jim will outline a timeline within two weeks.
- Pat wants to share the document (possibly just the table of contents) with ITMC as soon as possible to get the information out and to get more comments and feedback.
- Discussion occurred on differences in agencies and how the document would work individually for those agencies.
- Pat discussed the three tiers to document and what requirements would be for each organization. These would be tailored to your own group, etc.

RE: NIST Special Pub 800-39, 2.2 (pg 9) Multitiered Risk Management, addresses risk from a three-tiered approach beginning with Tier 1 as *Organization*, Tier 2 is *Business Processes*, and Tier 3 is *Information Systems*. Please contact Jim Ashmore or Pat Boles if you need assistance on how to document these three focuses or approaches for your group.

- Pat and Jim discussed timelines, milestones, and goals. Pat will update this information in the August folder.
- The document is included in the August meeting information on the ISMG SharePoint site.

Information Security Procurement/Acquisition Contract Language

- Jim reviewed the document he brought to share with the ISMG, discussed Information Security as part of RFPs and Contract Documents and recommended it be a part of "controls".
- Pat discussed Information Security Contracts and gave examples about awareness of the language. He wants all to review Jim's document [GENERAL COMMENTS to adding INFORMATION SECURITY to RFPs/Contract Documents] and we will discuss it in more depth at the next meeting.
- There was a brief discussion about contract language and the potential of adding additional language to the master contract.
- Pat will possibly bring Brett Boutin to an ISMG meeting at a later date to give more information on the topic.
- Kristi talked about perhaps the ISMG members could develop a list of questions for the discussion in our next meeting.

Updates

- Pat said the Security Standards on "Access Control" and "Identification and Authentication" are approved.
- Pat said the accounts for SANS have been set-up for about a month. Pat wants to know how it is working in everyone's systems by the next meeting.
- Pat said SANS doesn't allow you to be an administrator and a user but there is a work around by using a different email address. SANS will fix this issue in a future release.
- It was asked of Lynne what SITSD is doing in regards to the SANS training; if there is a pass/fail. Lynne says there are only a few questions on each topic that only take a few minutes so she is requiring all of the training and yes they have to pass. Lynne also says there is on-line new employee security training that is mandatory.

Other Business or Concerns – ISMG

- None

Adjourn – Pat Boles

****Action Item****

- The vote was unanimous. The meeting adjourned at 2:27 pm.